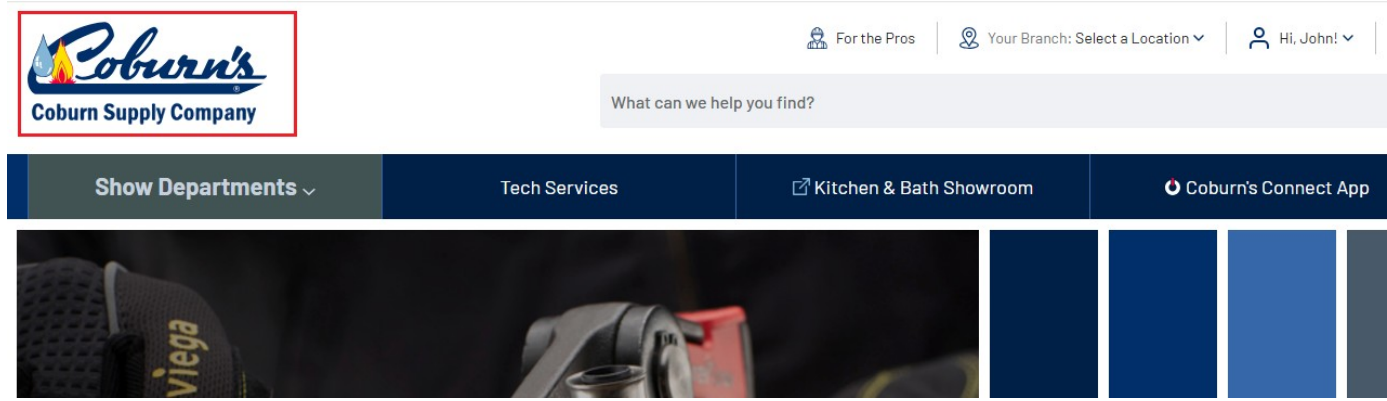# Exhibit 2

US8677116B1	Coburn Supply's website "coburns.com" ("The accused instrumentality")
1. A method of using a computer system to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer, the method comprising:	The accused instrumentality practices a method of using a computer system (e.g., authentication server of the accused instrumentality, etc.) to authenticate a user seeking to conduct at least one interaction (e.g., account login, product search, etc.) with a secured capability provided by a computer (e.g., server of the accused instrumentality). As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, product search, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access. https://www.coburns.com/

https://www.coburns.com/my-account/login?ReturnUrl=%2F

https://www.coburns.com/my-account

https://www.coburns.com/

Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by RapidSSL TLS RSA CA G1.

View certificate

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

https://www.coburns.com/

	Source: Fiddler capture of the accused instrumentality https://www.coburns.com/
using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;	The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a first signal (e.g., an AspNetCore.Identity.Application set response, etc.) from the computer (e.g., server of the accused instrumentality) providing the secured capability (e.g., secure connection with the website, etc.), the first signal comprising a reusable identifier (e.g., AspNetCore.Identity.Application, etc.) corresponding to the secured capability (e.g., secure connection with the website, etc.), the reusable identifier assigned for use by the secured capability for a finite period of time (e.g., Max-Age). As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is

achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, product search, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access. The server sends a response to set AspNetCore.Identity.Application value, which is set by the user device.

As shown, the AspNetCore.Identity.Application token set by the end device is reused in all further communications with the server. The AspNetCore.Identity.Application token also mentions a Max-Age (e.g., until session ends) for the token, indicating that it can be reused for a finite period.

https://www.coburns.com/

Security overview

🔒 ⓘ ⚠

This page is secure (valid HTTPS).

🔒 Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by RapidSSL TLS RSA CA G1.

View certificate

🔒 Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM.

🔒 Resources - all served securely

All resources on this page are served securely.

https://www.coburns.com/

Source: Fiddler captures of the accused instrumentality

https://www.coburns.com/

	Source: Fiddler Capture of the accused instrumentality Source: Fiddler Capture of the accused instrumentality
using the computer system to receive a second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information;	The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a second signal (e.g., a request signal from the user device) from an electronic device being used by the user, the second signal (e.g., request signal from the user device) comprising a copy of the reusable identifier (e.g., AspNetCore.Identity.Application, etc.) and user verification information (e.g., hjSessionUser_1256803). When the server sends a message containing an AspNetCore.Identity.Application to the user device, the client includes a copy of the AspNetCore.Identity.Application in all subsequent requests to the server, along with user verification information (e.g., hjSessionUser_1256803 credentials). This allows the server to authenticate the client for the duration of the session and ensure secure communication between the client and server.

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request Headers [Raw] [Header Definitions]

GET /ajax/locations HTTP/1.1

Cookies

⊟ Cookie   Reusable identifier

.AspNetCore.Antiforgery.mGU9TMToqzg=CfDJ8CJvvw5Nd71KsBm19ZP3r5BJ7tDF5vmn_dqo0r42gqr4dZNiHN5zBxvHTyWxQMknyrpSWSOnA9D-omN8jaD8yvjpMH2eHzbHTZ7q4

.AspNetCore.Identity.Application=CfDJ8CJvvw5Nd71KsBm19ZP3r5B1oHLp6-jo2RidygEJt71RsWfEi28XeCLXkS0lLABfBScck5XRcAaXkFXUjQ8pBo2HV1TEjbPGKkHMnRFsdTyE2O4kz

__cf_bm=QJRX0DihSitXvPp_Z4vzHlqVP3XkwinsVT98dsyeh6A-1732527515-1.0.1.1-e4YlcKTEijMbIffuY_48DQ2AejFEV0HzvpXJ9B.AiYHHqeul0GBKIX3WOhcAjcLZUVQF.UoE6W41.l

_ga_0ZC5BFST5D=GS1.1.1732527480.1.1.1732527674.33.0.0

_ga=GA1.1.324992762.1732527480

_gcl_au=1.1.2093780155.1732527480

Source: Fiddler Capture of the accused instrumentality

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request sent 2031 bytes of Cookie data:

__cf_bm=QJRX0DihSitXvPp_Z4vzHlqVP3XkwinsVT98dsyeh6A-1732527515-1.0.1.1-e4YlcKTEijMbIffuY_48DQ2AejFEV0HzvpXJ9B.AiYHHqeul0GBKIX3WOhcAjcLZUVQF.UoE6W41.FnYdYCVNA

_gcl_au=1.1.2093780155.1732527480

.AspNetCore.Antiforgery.mGU9TMToqzg=CfDJ8CJvvw5Nd71KsBm19ZP3r5BJ7tDF5vmn_dqo0r42gqr4dZNiHN5zBxvHTyWxQMknyrpSWSOnA9D-omN8jaD8yvjpMH2eHzbHTZ7q445cw-lmTJeX3SBx7ysG2Kw5kZeuMLksXxjKR262T6nOCJaEVN8

_ga=GA1.1.324992762.1732527480

cf_clearance=Km5iwmlPADuiE6rN6DGSM5bWN9GO0bhazvZE5Ln8T5o-1732527517-1.2.1.1-D5qMNv8tOtW89q.CZV5lMc4keAYEyfG5RdmdwlMCbELiSM9G4fVvXQE2saD1SOCcakFGEp.z7XJcA1qyXfailaA2qsMJ8bdLq3s48LuTBxFSQA1vAoHHGxoV.6JwSv21OICQ8Izwb1v4wyg2QwHPUfk25gykkkIWgv53rCnL67zJ_ERO4N9QPRVWcRvhv76ElLVG4hWLfY9A5dd8r9fX1hJT4maC1xeyM2TCm5CfWE6nmYtc2bJ6qCa3mVFp1b0Yj9opsgGyVcSPw0tmuR6yqbhk8IqE6Od1_pgTyfWaDauRoLc9CX03VT8zhy2EA43IqIw0AzABwxwFXcF3qpVcuHQEyIhG.MzSb.mPJPufZLZ09CHUVhJauM2shricEpD6

_hjSession_1256803=eyJpZCI6IjlhNGY1YzA4LWUyMTktNGM1ZS1iY2NjLTMxMzVkMmI1ZWNlOSIsImMiOjE3MzI1Mjc0ODE3MDMsInMiOjAsInIiOjAsInNiIjowLCJzciI6MCwic2UiOjAsImZzIjoxLCJzcCI6MH0=

_hjSessionUser_1256803=eyJpZCI6Ijg2ZGM0ODFmLThiOWMtNWI1NC04OWQzLWViNTAzMjA0ZGYxYiIsImNyZWF0ZWQiOjE3MzI1Mjc0ODE3MDEsImV4aXN0aW5nIjp0cnVlfQ==

.AspNetCore.Identity.Application=CfDJ8CJvvw5Nd71KsBm19ZP3r5B1oHLp6-jo2RidygEJt71RsWfEi28XeCLXkS0lLABfBScck5XRcAaXkFXUjQ8pBo2HV1TEjbPGKkHMnRFsdTyE2O4kzVIJ6RhS6boNpyNEnua_0UYNPl4vB7WZFW5n0PLlpjhM9xTK4p0zycOGdtDgto1CZBhmL7HxdLA3pyX33mQyalmCGpuXDVpNMGrrS-pEU5WG27IdJcysuhkZrstHh8pQKvNr7dpD86l29R-G08pOKujH93ySbx-q5ywj5OEKAA1PYHOs0mAVnoqsS1SiFwvWxHYmlPUR-HLHSbIOFzY-z9qdqkP3XwQVcusj3WyQJ98h6TLR2A9zjKzrg5opF5ZlVoiYNSq88KAfTuhqtXoYOohlKHmSUEm222kjiGA7HKFAVX_X3SKpyS2DAQdZ1vEphtA813PQ-phDukg3ckNM2Vpp4VL87b6Y0ERAhvs7tmppitKwPErWbzYCpNObhGnxFo6YqfxD4AKiO6SFDqGmjhStoAzwIrZS5bvxISRt386jNzDvIP8nP9MjsffX4LifDlC-TMu26gtVdPFl664_idyNAz0tV2EFqLNHfF7532xmYRawfuyfeVhuILJZZIP7ZLmAKWGs9Opz39vsMkbjt1-WZt-3OlD17JbL4eSb4fBjYkYKzfavWiHxadGvd_tjUmfGrFLIVHFy-kyZKNWeNABrbGwBLJ6lYn4jbO8VXmICEXquiMCUSKS7opTk

_ga_0ZC5BFST5D=GS1.1.1732527480.1.1.1732527674.33.0.0

the second signal comprising a copy of the reusable identifier

Source: Fiddler capture of the accused instrumentality

	Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
	
	D5qMNv8tOtW89q.CZV5lMc4keAYEyfG5RdmdwlMCbELiSM9G4fVvXQE2saD1SOCcakFGEp.z7XJcA1qyXfailaA2qsMJ8bdLq3s48LuTBxFSQA1vAoHHGxoV.6JwSv21OICQ8Izwb1v4
	wyg2QwHPUfk25gykkkIWgv53rCnL67zJ_ERO4N9QPRVWcRvhv76ElLVG4hWLfY9A5dd8r9fX1hJT4maC1xeyM2TCm5CfWE6nmYtc2bJ6qCa3mVFp1b0Yj9opsgGyVcSPw0tmuR6yq
	bhk8IqE6Od1_pgTyfWaDauRoLc9CX03VT8zhy2EA43IqIw0AzABwxwFXcF3qpVcuHQEyIhG.MzSb.mPJPufZLZ09CHUVhJauM2shricEpD6
	    _hjSession_1256803=
	
	    eyJpZCI6IjlhNGY1YzA4LWUyMTktNGM1ZS1iY2NjLTMxMzVkMmI1ZWNlOSIsImMiOjE3MzI1Mjc0ODE3MDMsInMiOjAsInIiOjAsInNiIjowLCJzciI6MCwic2UiOjAsImZzIjoxLC
	JzcCI6MH0= user verification information
	
	    _hjSessionUser_1256803=
	        eyJpZCI6Ijg2ZGM0ODFmLThiOWMtNWI1NC04OWQzLWViNTAzMjA0ZGYxYiIsImNyZWF0ZWQiOjE3MzI1Mjc0ODE3MDEsImV4aXN0aW5nIjp0cnVlfQ==
	
	Source: Fiddler capture of the accused instrumentality

using a processor of the computer system to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and	The accused instrumentality practices using a processor of the computer system (e.g., processor of the authentication server of the accused instrumentality, etc.) to evaluate, based at least on the first signal (e.g., an AspNetCore.Identity.Application set response, etc.) and the second signal (e.g., a request signal from the user device), whether the user is authorized to conduct the at least one interaction (e.g., account login, product search, etc.) with the secured capability (e.g., secure connection with the website, etc.). The server compares the reusable identifier, such as the token (e.g., AspNetCore.Identity.Application), in the first response received from the server with the token included in the client's subsequent request. If a match is found, the server authenticates the user and processes the request securely.

Source: Fiddler captures of the accused instrumentality

https://www.coburns.com/

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request sent 2031 bytes of Cookie data:

__cf_bm=QJRX0DihSitXvPp_Z4vzHlqVP3XkwinsVT98dsyeh6A-1732527515-1.0.1.1-e4YlcKTEijMbIffuY_48DQ2AejFEV0HzvpXJ9B.AiYHHqeul0GBKIX3WOhcAjcLZUVQF.UoE6W41.FnYdYCVNA

_gcl_au=1.1.2093780155.1732527480

.AspNetCore.Antiforgery.mGU9TMToqzg=CfDJ8CJvww5Nd71KsBm19ZP3r5BJ7tDF5vmn_dqo0r42gqr4dZNiHN5zBxvHTyWxQMknyrpSWSOnA9D-omN8jaD8yvjpMH2eHzbHTZ7q445cw-lmTJeX3SBx7ysG2Kw5kZeuMLksXxjKR262T6nOCJaEVN8

_ga=GA1.1.324992762.1732527480

cf_clearance=Km5iwmlPADuiE6rN6DGSM5bWN9GO0bhazvZE5Ln8T5o-1732527517-1.2.1.1-D5qMNv8tOtW89q.CZV5lMc4keAYEyfG5RdmdwlMCbELiSM9G4fVvXQE2saD1SOCcakFGEp.z7XJcA1qyXfailaA2qsMJ8bdLq3s48LuTBxFSQA1vAoHHGxoV.6JwSv21OICQ8Izwb1v4wyg2QwHPUfk25gykkkIWgv53rCnL67zJ_ERO4N9QPRVWcRvhv76ElLVG4hWLfY9A5dd8r9fX1hJT4maC1xeyM2TCm5CfWE6nmYtc2bJ6qCa3mVFp1b0Yj9opsgGyVcSPw0tmuR6yqbhk8IqE6Od1

_pgTyfWaDauRoLc9CX03VT8zhy2EA43IqIw0AzABwxwFXcF3qpVcuHQEyIhG.MzSb.mPJPufZLZ09CHUVhJauM2shricEpD6

_hjSession_1256803=
            eyJpZCI6IjlhNGY1YzA4LWUyMTktNGM1ZS1iY2NjLTMxMzVkMmI1ZWNlOSIsImMiOjE3MzI1Mjc0ODE3MDMsInMiOjAsInIiOjAsInNiIjowLCJzciI6MCwic2UiOjAsImZzIjoxLCJzcCI6MH0=

_hjSessionUser_1256803=
            eyJpZCI6Ijg2ZGM0ODFmLThiOWMtNWI1NC04OWQzLWViNTAzMjA0ZGYxYiIsImNyZWF0ZWQiOjE3MzI1Mjc0ODEsImV4aXN0aW5nIjp0cnVlfQ==

.AspNetCore.Identity.Application=CfDJ8CJvww5Nd71KsBm19ZP3r5B1oHLp6-jo2RidygEJt71RsWfEi28XeCLXkS0lLABfBScck5XRcAaXkFXUjQ8pBo2HV1TEjbPGKkHMnRFsdTyE2O4kzVIJ6RhS6boNpyNEnua_0UYNPl4vB7WZFW5n0PLlpjhM9xTK4p0zycOGdtDgto1CZBhmL7HxdLA3pyX33mQyalmCGpuXDVpNMGrrS-pEU5WG27IdJcysuhkZrstHh8pQKvNr7dpD86l29R-G08pOKujH93ySbx-q5ywj5OEKAA1PYHOs0mAVnoqsS1SiFwvWxHYmlPUR-HLHSbIOFzY-z9qdqkP3XwQVcusj3WyQJ98h6TLR2A9zjKzrg5opF5ZlVoiYNSq88KAfTuhqtXoYOohlKHmSUEm222kjiGA7HKFAVX_X3SKpyS2DAQdZ1vEphtA813PQ-phDukg3ckNM2Vpp4VL87b6Y0ERAhvs7tmppitKwPErWbzYCpNObhGnxFo6YqfxD4AKiO6SFDqGmjhStoAzwIrZS5bvxISRt386jNzDvIP8nP9MjsffX4LifDlC-TMu26gtVdPFl664_idyNAz0tV2EFqLNHfF7532xmYRawfuyfeVhuILJZZIP7ZLmAKWGs9Opz39vsMkbjt1-WZt-3OlD17JbL4eSb4fBjYkYKzfavWiHxadGvd_tjUmfGrFLIVHFy-kyZKNWeNABrbGwBLJ6lYn4jbO8VXmICEXquiMCUSKS7opTk

_ga_0ZC5BFST5D=GS1.1.1732527480.1.1.1732527674.33.0.0

the second signal comprising a copy of the reusable identifier

Source: Fiddler capture of the accused instrumentality

[Coburn's — Coburn Supply Company]

For the Pros | Your Branch: Select a Location ⌄ | Hi, John! ⌄

What can we help you find?

Show Departments ⌄ | Tech Services | Kitchen & Bath Showroom | Coburn's Connect App

https://www.coburns.com/

https://www.coburns.com/my-account/login?ReturnUrl=%2F

https://www.coburns.com/

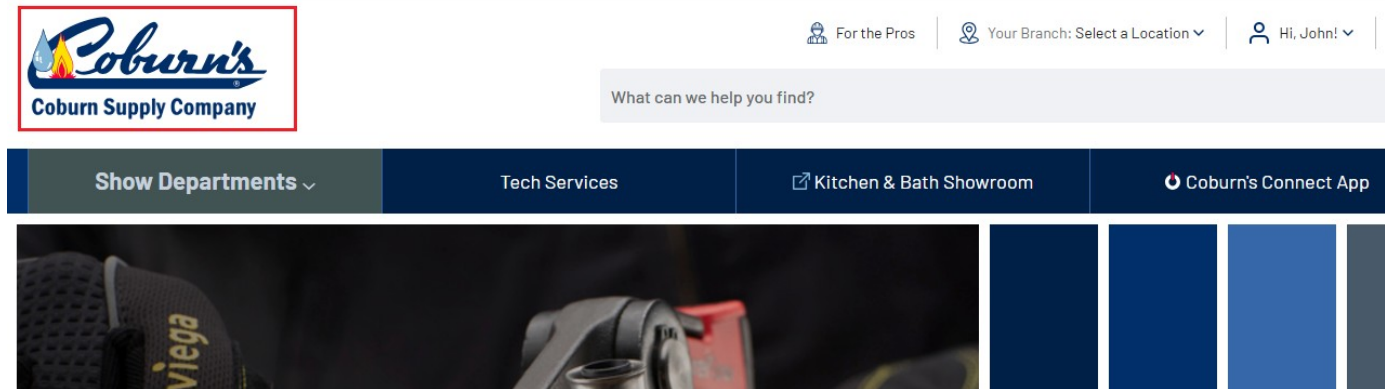|	
	Security overview 🔒 ⓘ ⚠ **This page is secure (valid HTTPS).** 🔒 Certificate - valid and trusted The connection to this site is using a valid, trusted server certificate issued by RapidSSL TLS RSA CA G1. View certificate 🔒 Connection - secure connection settings The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM. 🔒 Resources - all served securely All resources on this page are served securely. https://www.coburns.com/
in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, using the computer system to transmit a third signal comprising authorization	The accused instrumentality practices in response to an indication from the processor (e.g., processor of the authentication server of the accused instrumentality, etc.) that the user is authorized to conduct the at least one interaction with the secured capability (e.g., secure connection with the website, etc.), using the computer system processor (e.g., authentication server of the accused instrumentality, etc.) to transmit a third signal comprising authorization information (e.g., a response signal from the server to the user device, etc.) to at least one of the electronic device (e.g., user device, etc.) and the computer.

information to at least one of the electronic device and the computer.	As shown, upon authenticating the AspNetCore.Identity.Application, the user device receives an authentication confirmation message (a third signal), from the server to the user device.
	Source: Fiddler capture of the accused instrumentality
	https://www.coburns.com/